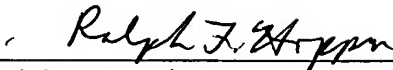


Entry of this amendment is respectfully requested.

Respectfully submitted,

Dated: 2/28/02



Ralph F. Hoppin, Reg. No. 38,494
Attorney for Applicants
BROWN RAYSMAN MILLSTEIN FELDER &
STEINER LLP
900 Third Avenue
New York, New York 10022
(212) 895-2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : SAKUSHIMA et al.
Application No. :
Filed : herewith
Title : USER INFORMATION MANAGEMENT
APPARATUS

BOX PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

**AMENDED CLAIMS MARKED UP TO SHOW CHANGES RELATIVE TO
PREVIOUS VERSION (37 CFR 1.121(c)(ii))**

In the marked up claims below, new text is underlined and deleted text is
lined out.

5. A user information management apparatus according to ~~any one of claims 1 to 4,~~claim 1, wherein said user identifying means determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and said level determining means determines that the certification level is the lowest.

6. A user information management apparatus according to ~~any one of claims 1 to 5,~~claim 1, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control means instructs the user to take action required to level up to the required certification level.

7. A user information management apparatus according to ~~any one of claims 1 to 6,~~claim 1, wherein said transmission control means has means for defining a security level specific to said user information and means for managing said user information for said each security level.

8. A user information management apparatus according to ~~any one of claims 1 to 7,~~claim 1, wherein the apparatus is arranged to hold, in the storage means, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

9. A user information management apparatus according to ~~any one of claims 1 to 8,~~claim 1, wherein, for a set of requested data, an index as an ID is obtained from a distance between a probability of such an event and data, and then, the obtained value is used to reconfirm a security.

10. A user information management apparatus according to ~~any one of claims 1 to 9,~~claim 1 wherein the apparatus is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining means is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

14. A user information management apparatus according to ~~any one of claims 1 to 13,~~ wherein said transmission control means further comprises a user information use criterion storing means for storing a user information use criterion for a data requester in advance and a user information providing condition storing means for storing a user information providing condition for a data provider in advance, and, when the user information use criterion and the user information providing condition are compared with each other, and transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

18. A user information management method according to ~~any one of claims 15 to 17,~~claim 15, wherein said level determining step determines a predetermined technique employed by the user for the purpose of user identification, thereby determining a level.

19. A user information management method according to ~~any one of claims 15 to 18,~~claim 15, wherein said user identifying step determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and, in this case, said level determining step determines that the certification level is the lowest.

20. A user information management method according to ~~any one of claims 15 to 19,~~claim 15, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control step instructs the user to take action required to level up to the required certification level.

21. A user information management method according to ~~any one of claims 15 to 20,~~claim 15, wherein said transmission control step has the step of defining a security level specific to said user information and the step of managing said user information for said each security level.

22. A user information management method according to ~~any one of claims 15 to 21,~~claim 15, wherein the method is arranged to hold, in the storage step, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

23. A user information management method according to ~~any one of claims 15 to 22,~~claim 15, wherein the method comprises the step of obtaining, for a set of requested data, an index as an ID from a distance between a probability of such an event and data, and then using the obtained value to reconfirm a security.

24. A user information management method according to ~~any one of claims 15 to 23,~~claim 15, wherein the method is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining step is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

28. A user information management method according to ~~any one of claims 15 to claim 27, 15,~~ wherein, a user information use criterion for a data requester is stored in advance, and a user information providing condition for a data provider is stored in advance, and when the transmission control step further compares the user information use criterion and the user information providing condition with each other, so that transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

32. A recording medium having recorded in a computer readable state a control program for executing the user information management method according to ~~any one of claims 29 and 31,~~ claim 29, wherein said level determining step determines a predetermined technique employed by the user for the purpose of user identification, thereby determining a level.

33. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 32,~~ claim 29, wherein said user identifying step determines said user based on a predetermined instruction from an input device operated by said user at said user terminal, and, in this case, said level determining step determines that the certification level is the lowest.

34. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 33,~~ claim 29, wherein, if a current certification level of the user is lower than a desired certification level required for data acquisition, said transmission control step instructs the user to take action required to level up to the required certification level.

35. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 34~~, claim 29, wherein said transmission control step has the step of defining a security level specific to said user information and the step of managing said user information for said each security level.

36. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 35~~, claim 29, wherein the recording medium is arranged to hold, in the storage step, information common to a plurality of users who use the user terminals as group data to be associated with a security level.

37. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 36~~, claim 29, wherein the recording medium is arranged so that, for a set of requested data, an index as an ID is obtained from a distance between a probability of such an event and data, and then, the obtained value is used to reconfirm a security.

38. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 and 37~~, claim 29, wherein the recording medium is arranged so that said plurality of user terminals are classified in advance into a plurality of security divisions, and security division determining step is provided, thereby applying access restriction for such each security division of the user terminal that has made access.

42. A recording medium having recorded in a computer readable state a control program for executing the user information managing method according to ~~any one of claims 29 to 41~~, claim 29, wherein the recording medium is arranged so that, a user information use criterion for a data requester is stored in advance, and a user information providing condition for a data provider is stored in advance, and when the user information use criterion and the user information providing condition are compared with each other, and transmission is controlled based on the comparison result, if user information other than that on a user determined by the user determination means is contained in data, the user information providing condition of the user is obtained, and comparison with the user information use criterion is carried out, thereby determining whether or not transmission is carried out.

Respectfully submitted,

Ralph F. Hoppin 2/28/02
Ralph F. Hoppin, Reg. No. 38,494
BROWN RAYSMAN MILLSTEIN
FELDER & STEINER, LLP
900 Third Avenue
New York, NY 10022
Tel. (212) 895-2000
Fax (212) 895-2900